ABSTRACT OF THE DISCLOSURE

A pre-computation and dual-pass modular operation approach to implement encryption protocols efficiently in electronic integrated circuits is disclosed. An encrypted electronic message is received and another electronic message generated based on the encryption protocol. Two passes of Montgomery's method are used for a modular operation that is associated with the encryption protocol along with pre-computation of a constant based on a modulus. The modular operation may be a modular multiplication or a modular exponentiation. Modular arithmetic may be performed using the residue number system (RNS) and two RNS bases with conversions between the two RNS bases. A minimal number of register files are used for the computations along with an array of multiplier circuits and an array of modular reduction circuits. The approach described allows for high throughput for large encryption keys with a relatively small number of logical gates.